UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/400,442	09/21/1999	JEAN-CLAUDE SARFATI	1581.0380001	3447

7590 10/06/2003

STERNE KESSLER GOLDSTEIN & FOX P.L.L.C.
ATTORNEYS AT LAW
1100 NEW YORK AVENUE N.W.
SUITE 600
WASHINGTON, DC 20005-3934

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2131	9

DATE MAILED: 10/06/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/400,442	SARFATI ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☒ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *7, 8* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-53 have been examined and rejected under of 35 U.S.C. 102(b).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. ***Claims 1-53 are rejected under 35 U.S.C. 102(b) as being unpatentable by Rohatgi, et al. (US 5,625,693).***

As per claim 1:

Rohatgi, et al. teaches a measure to assure protection of ITVS receivers from unauthorized data potential disruption (col.1, lines 11-65) wherein includes downloading and (video/audio) compression standard promoted by MPEG (col.3, lines 1-34). Rohatgi discloses the formation of the applications where the portions of the programs are formatted into modules and divided into transmission units (col.3, line 61-col.4, line 4).

Rohatgi discusses a plurality of modules such as Directory Module, Code Module, and Data Module (col.4, lines 10-25). There includes Table I and Table II, wherein Table I illustrates types of information included in each header packet where the header includes a version number to indicate when there is a change made. Table II illustrates the types of data included in the

Directory Module wherein contains a header with an Application identifier (AID), a field indicating application type, a field which includes type qualifiers, a field which indicates the amount of memory required to store and execute the application, a field indicating the number of modules contained in the application, and field(s) which include security data (authentication data) (col.4, lines 34-40). In addition, there is a string table listing the respective application module names in ASCII format. The Examiner asserts that it is inherent Rohatgi includes extensions (ID) located in the field indicating application type (col.8, lines 4-12) wherein the Examiner further asserts that a program or a user assigns extensions, hence, the use of extensions would be to identify (the modules/table) as a member of a category wherein that category may contain the same type of extension, which is the same type of module/table (col.4, lines 50-66). Rohatgi discloses the directory table and module tables are transmitted in an MPEG bitstream (col.3, lines 12-26) where at the receiver decoder for receiving MPEG bitstream (col.4, lines 40-41).

Rohatgi discloses downloading one of the Directory (MPEG) modules having the predetermined TID extension of the module MPEG tables (col.16, lines 50-66) and to determine from the content of the Directory module the extensions of the module tables (col.6, lines 22-42) whether the module is determined to be the Directory module (col.10, lines 42-50). Also see Figure 4.

As per claim 2:

As rejected in claim 1 and Rohatgi further discloses the receiver decoder detects if there is a change in version number (col.4, lines 37-42). Also see col.17, lines 13-18.

As per claim 3:

Rohatgi discusses a module being divided into transmission units to facilitate interleaving of information from different modules (col.4, lines 2-4) wherein there includes a field indicating the number of modules and data section (col.4, lines 54-66). Also, see Figure 5.

As per claim 4:

Rohatgi discusses processing means for downloading the MPEG tables with its extension to storage means (col.14, lines 24-44) wherein the packets are loaded into respective predetermined memory locations. See also Figures 8, 9, and 11.

As per claim 5:

As rejected in claim 4 and further Rohatgi discloses the receiver decoder detects if there is a change in version number (col.4, lines 37-42) and restarting the process (col.16, line 1). Also see col.17, lines 13-18.

As per claim 6:

Rohatgi discloses a test to determine if a complete module has been loaded (col.15, lines 54-61).

As per claim 7: See col.2, lines 48-54; discussing the port that is arranged to receive an application. Also see FIG.1

As per claim 8:

Rohatgi discloses means for dividing into a plurality of modules an application to be downloaded to a receiver decoder (col.3, line 55-col.4, line 4) and formatting the modules as respective table that has the same identification and respective different (ID) extension (col., lines 33-66).

As per claim 9: See col.4, lines 37-42; discussing the version number.

As per claim 10:

Rohatgi discusses a module being divided into transmission units to facilitate interleaving of information from different modules (col.4, lines 2-4) wherein there includes a field indicating the number of modules and data section (col.4, lines 54-66). Also, see Figure 5.

As per claim 11:

Rohatgi discloses generating a signature for the data (col.5, lines 46-65) to be downloaded and encrypting the signature using a private key (col.8, lines 37-66). See also col.10, lines 35-67. Further, Rohatgi discusses transmitting the Directory module with the signature that includes a flag that is designated to select one of the public keys that should be use to decrypt (col.6, lines 22-42) to provide a decrypted signature wherein is used to compare with the signature generated at the receiver decoder (col.16, lines 7-26).

As per claim 12:

Rohatgi teaches generating a signature for the data (col.5, lines 46-65) to be downloaded and encrypting the signature using a private key that has a predetermined key identification and running the Application at the receiver/decoder to receive a further key (col.8, lines 37-66). See also col.10, lines 35-67.

As per claim 13: See col.16, lines 9-19.

As per claim 14: See col.7, lines 45-46.

As per claim 15:

See col.6, lines 45-59 and col.11, lines 48-53; discussing validation flag for the selected public key. Also see col.16, lines 3-4. Rohatgi teaches discarding or aborting downloading the generated module if the generated module is not authentic wherein the Examiner asserts does not match to the respective Directory module (col.15, lines 43-46).

As per claim 16: See col.12, lines 23-67; discussing changing and the ability to receive such a further key is determined in dependence upon the state of the validation flag.

As per claim 17:

Rohatgi discloses generating a signature for the data (col.5, lines 46-65) to be downloaded and encrypting the signature using a private key (col.8, lines 37-66). See also col.10, lines 35-67. Further, Rohatgi discusses transmitting the Directory module with the signature that includes a flag that is designated

to select one of the public keys that should be use to decrypt (col.6, lines 22-42) to provide a decrypted signature wherein is used to compare with the signature generated at the receiver decoder (col.16, lines 7-26). Rohatgi discusses a validation flag for the selected public key (col.6, lines 45-59 and col.11, lines 48-53) that has a corresponding private key.

As per claim 18: See col.11, lines 13 thru col.12, line 38; discussing encrypting and comparing the validation code with the signature.

As per claim 19:

Rohatgi discuss generating a validation flag (col.6, lines 45-59 and col.11, lines 48-53) and generating a signature wherein encrypting and comparing the validation code with the signature with a private key (col.11, lines 13 thru col.12, line 38). Also see col.16, lines 3-4. Rohatgi teaches discarding or aborting downloading the generated module if the generated module is not authentic wherein the Examiner asserts does not match to the respective Directory module (col.15, lines 43-46).

As per claim 20: See col.16, lines 3-4 and col.15, lines 43-46; discussing aborting downloading the data.

As per claim 21:

As rejected with the same rationale as in claim 11, but differs by including an offset of a data block and a signature. Rohatgi discuss the Table I, which includes a Module Transmission Unit Byte Offset to indicate the location in the module of the payload (col.4, lines 44-48). Rohatgi restarts

(repeats) the steps of look-up, extracting, and comparing the signature (col.15, line 60 thru col.16, line 67). See also Figure 5.

As per claim 22:

Rohatgi discloses generating a signature for the data (col.5, lines 46-65) to be downloaded and encrypting the signature using a private key (col.8, lines 37-66). See also col.10, lines 35-67. Further, Rohatgi discusses transmitting the Directory module with the signature that includes a flag that is designated to select one of the public keys that should be use to decrypt (col.6, lines 22-42) to provide a decrypted signature wherein is used to compare with the signature generated at the receiver decoder (col.16, lines 7-26). Rohatgi includes a Module Transmission Unit Byte Offset to indicate the location in the module of the payload (col.4, lines 44-48). The Examiner asserts an offset indicates where the starting point of a particular item is located (i.e. a relative address).

As per claim 23:

Rohatgi the extracted signature and the generated signature are compared (col.5, line 42 thru col.6, line 40). See also col.12, line 41 thru col.13, line 23. Rohatgi discuss the Table I, which includes a Module Transmission Unit Byte Offset to indicate the location in the module of the payload (col.4, lines 44-48). Rohatgi restarts (repeats) the steps of look-up, extracting, and comparing the signature (col.15, line 60 thru col.16, line 67). See also Figure 5.

As per claim 24: See col.4, lines 2-29.

As per claim 25:

Rohatgi discloses the directory table and module tables are transmitted in an MPEG bitstream (col.3, lines 12-26) where at the receiver decoder for receiving MPEG bitstream (col.4, lines 40-41).

Rohatgi teaches downloading one of the Directory (MPEG) modules having the predetermined TID extension of the module MPEG tables (col.16, lines 50-66). Also see Figure 4. Rohatgi discloses generating a signature for the data (col.5, lines 46-65) to be downloaded and encrypting the signature using a private key (col.8, lines 37-66). See also col.10, lines 35-67. Further, Rohatgi discusses transmitting the Directory module with the signature that includes a flag that is designated to select one of the public keys that should be use to decrypt (col.6, lines 22-42) to provide a decrypted signature wherein is used to compare with the signature generated at the receiver decoder (col.16, lines 7-26).

As per claim 26:

Rohatgi teaches generating a signature for the data (col.5, lines 46-65) to be downloaded and encrypting the signature using a private key (col.8, lines 37-66). See also col.10, lines 35-67. Further, Rohatgi discusses transmitting the Directory module with the signature that includes a flag that is designated to select one of the public keys that should be use to decrypt (col.6, lines 22-

42) to provide a decrypted signature wherein is used to compare with the signature generated at the receiver decoder (col.16, lines 7-26).

Rohatgi discloses the formation of the applications where the portions of the programs are formatted into modules and divided into transmission units (col.3, line 61-col.4, line 4) and includes a plurality of modules such as Directory Module, Code Module, and Data Module (col.4, lines 10-25).

As per claim 27:

Rohatgi teaches discarding or aborting downloading the generated module if the generated module is not authentic wherein the Examiner asserts does not match to the respective Directory module (col.15, lines 43-46).

As per claim 28:

Rohatgi teaches if the generated signature is not authentic (or comparable) to the decrypted signature, then discarding or aborting downloading the data (col.15, lines 43 thru col.16, lines 66).

As per claim 29:

Rohatgi include MPEG tables and means for storing public keys and identification (col.FIG.1). Rohatgi further teaches generating a signature for the data (col.5, lines 46-65) to be downloaded and encrypting the signature using a private key that has a predetermined key identification and transmits the signature with public key of the Directory module for decryption (col.6, lines 22-42) wherein to provide a decrypted signature which is use to compare with the signature generated at the receiver decoder (col.16, lines 7-26).

As per claim 30: See col.15, lines 20-25 and Figure 9; discusses the key storing means is provided by the ROM.

As per claim 31: See col.6, lines 22-39.

As per claim 32:

Rohatgi teaches generating a signature for the data (col.5, lines 46-65) to be downloaded and encrypting the signature using a private key that has a predetermined key identification and running the Application at the receiver/decoder to receive a further key (col.8, lines 37-66). See also col.10, lines 35-67.

As per claim 33: See col.16, lines 7-10 discussing the further key being stored in the volatile memory.

As per claim 34: See col.6, lines 63-67.

As per claim 35: See col.15, lines 20-21 discussing RAM.

As per claim 36:

Rohatgi teaches discarding or aborting downloading it is proven to not be authentic (col.15, lines 43-46). The Examiner asserts it is inherent that proving authenticity can be one of amongst many ways, for instance, comparing if the generated signature with the decrypted signature or generated signature to its respective signature of a directory or if validation code is not set.

As per claim 37: See col.12, lines 23-67; discussing changing and the ability to receive such a further key is determined in dependence upon the state of the validation flag.

As per claim 38:

Rohatgi discloses means for storing a public key and an identification of the public key (see FIG.9) and in addition Rohatgi includes a public key flag (col.6, lines 22-42). See col.6, lines 45-59 and col.11, lines 48-53; discussing validation flag for the selected public key. Rohatgi discusses transmitting the Directory module with the signature that includes a flag that is designated to select one of the public keys that should be use to decrypt (col.6, lines 22-42) to provide a decrypted signature wherein is used to compare with the signature generated at the receiver decoder (col.16, lines 7-26). See also col.13, lines 38-44.

As per claim 39: See col.15, lines 18-26; discussing rewritable non-volatile memory.

As per claim 40: See col.6, lines 45-59 and col.11, line 48 thru col.12, line 24; discussing validation flag within a memory are arranged as a bitmap. See Figures 3, 5, and 6.

As per claim 41: See col.6, lines 45-59 and col.11, line 48 thru col.12, line 24; discussing decrypting the validation code and comparing the validation code with the decrypted validation code.

As per claim 42: As rejected with the same rationale as applied in claim 19.

As per claim 43:

Rohatgi teaches discarding or aborting downloading it is proven to not be authentic (col.15, lines 43-46). The Examiner asserts it is inherent that proving authenticity can be one of amongst many ways, for instance, comparing if the generated signature with the decrypted signature or generated signature to its respective signature of a directory or if validation code is not set or matched.

As per claim 44: See col.15, lines 18-26; discussing rewritable non-volatile memory.

As per claim 45: See col.6, lines 45-59 and col.11, line 48 thru col.12, line 24; discussing validation flag within a memory are arranged as a bitmap. See Figures 3, 5, and 6.

As per claim 46:

Rohatgi discuss the Table I, which includes a Module Transmission Unit Byte Offset to indicate the location in the module of the payload (col.4, lines 44-48). Rohatgi includes the steps of look-up a stored offset, extracting the signature from the decrypted data block using the looked-up offset (col.15, line 60 thru col.16, line 67). See also Figure 5.

As per claim 47:

Rohatgi discloses generating a signature for the data (col.5, lines 46-65) to be downloaded and encrypting the signature using a private key (col.8, lines 37-66). See also col.10, lines 35-67. Further, Rohatgi discusses transmitting

the Directory module with the signature that includes a public key for decrypting (col.6, lines 22-42) and to provide a decrypted signature wherein is used to compare with the signature generated at the receiver decoder (col.16, lines 7-26). Rohatgi includes a Module Transmission Unit Byte Offset to indicate the location in the module of the payload (col.4, lines 44-48). The Examiner asserts an offset indicates where the starting point of a particular item is located (i.e. a relative address).

As per claim 48:

Rohatgi discuss the Table I, which includes a Module Transmission Unit Byte Offset to indicate the location in the module of the payload (col.4, lines 44-48). Rohatgi restarts (repeats) the steps of look-up, extracting, and comparing the signature (col.15, line 60 thru col.16, line 67). See also Figure 5.

As per claim 49: See col.15, lines 18-26; discussing rewritable non-volatile memory.

As per claim 50:

Rohatgi discloses generating a signature for the data (col.5, lines 46-65) to be downloaded and encrypting the signature using a private key (col.8, lines 37-66). See also col.10, lines 35-67. Further, Rohatgi discusses transmitting the Directory module with the signature that includes a public key for decrypting (col.6, lines 22-42) and to provide a decrypted signature wherein is

used to compare with the received signature with the respective signature generated at the receiver decoder (col.16, lines 7-67).

As per claim 51:

Rohatgi discloses the directory table and module tables are transmitted in an MPEG bitstream (col.3, lines 12-26) where at the receiver decoder for receiving MPEG bitstream (col.4, lines 40-41).

Rohatgi teaches downloading one of the Directory (MPEG) modules having the predetermined TID extension of the module MPEG tables (col.16, lines 50-66). Also see Figure 4. Rohatgi discloses generating a signature for the data (col.5, lines 46-65) to be downloaded and encrypting the signature using a private key (col.8, lines 37-66). See also col.10, lines 35-67. Further, Rohatgi discusses transmitting the Directory module with the signature that includes one of the public keys stored of the memory for decryption (col.6, lines 22-42), and to provide a decrypted signature wherein is used to compare with the received signature with the respective signature generated at the receiver decoder (col.16, lines 7-67).

As per claim 52:

Rohatgi teaches discarding or aborting downloading the generated module if the generated module is not authentic wherein the Examiner asserts does not match to the respective Directory module.

As per claim 53:

Rohatgi teaches if the generated signature is not authentic (or comparable) to the decrypted signature, then discarding or aborting downloading the data (col.15, lines 43 thru col.16, lines 66).

Conclusion

For further details and description of the above rejections, see Figures 1-12 and col.2, line 48. ET SEQ.

3. ***The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.***

Satterfield (US 5,717,760)

Rakavy, Et. Al. (US 6,324,644)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (703) 305-3853. The examiner can normally be reached on Monday - Friday (7:00 - 3:30PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ SHEIKH can be reached on (703) 305-9648. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5631.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

LHA
September 27, 2003